ELLIPTIC CURVES CRYPTOGRAPHY

FRANCESCO PAPPALARDI

#1 - FIRST LECTURE.

SEPTEMBER 14TH 2015

National University of Mongolia
Ulan Baatar, Mongolia
September 14, 2015

Three Lectures on Elliptic Curves Cryptography

Note (Program of the Lectures)

1. Generalities on Elliptic Curves over finite Fields
2. Basic facts on Discrete Logarithms on finite groups, generic attacks (Pohlig–Hellmann, BSGS, Index Calculus)
3. Elliptic curves Cryptography: pairing based Cryptography, MOV attacks, anomalous curves

Notations

Fields of characteristics 0

1. $\mathbb{Q}$ is the field of rational numbers
2. $\mathbb{R}$ and $\mathbb{C}$ are the fields of real and complex numbers
3. $K \subset \mathbb{C}$, $\dim_{\mathbb{Q}} K < \infty$ is a *number field*
   - $\mathbb{Q}[\sqrt{d}]$, $d \in \mathbb{Q}$
   - $\mathbb{Q}[\alpha]$, $f(\alpha) = 0$, $f \in \mathbb{Q}[X]$ irreducible

Finite fields

1. $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ is the prime field;
2. $\mathbb{F}_q$ is a finite field with $q = p^n$ elements
3. $\mathbb{F}_q = \mathbb{F}_p[\xi]$, $f(\xi) = 0$, $f \in \mathbb{F}_p[X]$ irreducible, $\partial f = n$
4. $\mathbb{F}_4 = \mathbb{F}_2[\xi]$, $\xi^2 = 1 + \xi$
5. $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, $\alpha^3 = \alpha + 1$ but also $\mathbb{F}_8 = \mathbb{F}_2[\beta]$, $\beta^3 = \beta^2 + 1$, $(\beta = \alpha^2 + 1)$
6. $\mathbb{F}_{101^{101}} = \mathbb{F}_{101}[\omega]$, $\omega^{101} = \omega + 1$

Notations

Algebraic Closure of $\mathbb{F}_q$

- $\mathbb{C} \supset \mathbb{Q}$ satisfies that *Fundamental Theorem of Algebra*! (i.e. $\forall f \in \mathbb{Q}[x], \partial f > 1, \exists \alpha \in \mathbb{C}, f(\alpha) = 0$)
- We need a field that plays the role, for $\mathbb{F}_q$, that $\mathbb{C}$ plays for $\mathbb{Q}$. It will be $\overline{\mathbb{F}_q}$, called *algebraic closure of* $\mathbb{F}_q$

1. $\forall n \in \mathbb{N}$, we fix an $\mathbb{F}_{q^n}$
2. We also require that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if $n \mid m$
3. We let $\overline{\mathbb{F}_q} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{q^n}$

- **Fact:** $\overline{\mathbb{F}_q}$ is *algebraically closed*
  (i.e. $\forall f \in \mathbb{F}_q[x], \partial f > 1, \exists \alpha \in \overline{\mathbb{F}_q}, f(\alpha) = 0$)

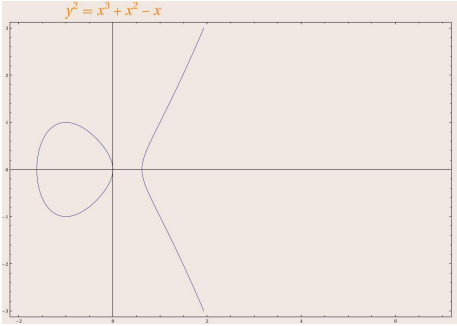
If $F(x, y) \in \mathbb{Q}[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \mathbb{C}^2$ s.t. $F(x_0, y_0) = 0$.
If $F(x, y) \in \mathbb{F}_q[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \overline{\mathbb{F}_q}^2$ s.t. $F(x_0, y_0) = 0$.

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



The equation should not be *singular*

The Discriminant of an Equation

The condition of absence of singular points in terms of a_1, a_2, a_3, a_4, a_6

Definition

The *discriminant* of a Weierstraß equation over $\mathbb{F}_q$, $q = p^n$, $p \geq 3$ is

$$\begin{aligned}\Delta_E := \frac{1}{2^4}\Big(&-a_1^5a_3a_4 - 8a_1^3a_2a_3a_4 - 16a_1a_2^2a_3a_4 + 36a_1^2a_3^2a_4\\ &- a_1^4a_4^2 - 8a_1^2a_2a_4^2 - 16a_2^2a_4^2 + 96a_1a_3a_4^2 + 64a_4^3 +\\ &a_1^6a_6 + 12a_1^4a_2a_6 + 48a_1^2a_2^2a_6 + 64a_2^3a_6 - 36a_1^3a_3a_6\\ &-144a_1a_2a_3a_6 - 72a_1^2a_4a_6 - 288a_2a_4a_6 + 432a_6^2\Big)\end{aligned}$$

Note

E is *non singular* if and only if $\Delta_E \neq 0$

Special Weierstraß equation of $E/\mathbb{F}_{p^\alpha}$, $p \neq 2$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \mathbb{F}_{p^\alpha}$$

If we "complete the squares" by applying the

$$\begin{cases} x \leftarrow x \\ y \leftarrow y - \frac{a_1x + a_3}{2} \end{cases}$$

transformation:
the Weierstraß equation becomes:

$$E' : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

where $a_2' = a_2 + \frac{a_1^2}{4}$, $a_4' = a_4 + \frac{a_1a_3}{2}$, $a_6' = a_6 + \frac{a_3^2}{4}$
If $p \geq 5$, we can also apply the transformation

$$\begin{cases} x \leftarrow x - \frac{a_2'}{3} \\ y \leftarrow y \end{cases}$$

obtaining the equations:

$$E'' : y^2 = x^3 + a_4''x + a_6''$$

where $a_4'' = a_4' - \frac{a_2'^2}{3}$, $a_6'' = a_6' + \frac{2a_2'^3}{27} - \frac{a_2'a_4'}{3}$

Definition

Two Weierstraß equations over $\mathbb{F}_q$ are said (affinely) equivalent if there exists a (affine) change of variables that takes one into the other

Note

The only affine transformation that take a Weierstrass equations in another Weierstrass equation have the form

$$\begin{cases} x \longleftarrow u^2x + r \\ y \longleftarrow u^3y + u^2sx + t \end{cases} \qquad r, s, t, u \in \mathbb{F}_q$$

The Weierstraß equation

Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/\mathbb{F}_q (q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 5	$4A^3 + 27B^2$
$y^2 + xy = x^3 + a_2x^2 + a_6$	2	a_6^2
$y^2 + a_3y = x^3 + a_4x + a_6$	2	a_3^4
$y^2 = x^3 + Ax^2 + Bx + C$	3	$4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2$

Definition (Elliptic curve)

An elliptic curve is the data of a non singular Weierstraß equation (i.e. $\Delta_E \neq 0$)

Note: If $p \geq 3$, $\Delta_E \neq 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has no double root

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

However the change of variables $\begin{cases} x \leftarrow x + 1 \\ y \leftarrow y + x \end{cases}$ takes the sixth curve into the fifth. Hence we can remove the sixth from the list.

Fact:

There are 5 affinely inequivalent elliptic curves over $\mathbb{F}_2$

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Fact:

let $\left(\frac{a}{q}\right)$ be the Kronecker symbol. Then the number of non–isomorphic (i.e. inequivalent) classes of elliptic curves over $\mathbb{F}_q$ is

$$2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$$

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve and consider a "symbol" ∞ (point at infinity). Set

$$E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

Hence

- $E(\mathbb{F}_q) \subset \mathbb{F}_q^2 \cup \{\infty\}$
- If $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, then $E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^n})$
- We may think that ∞ sits on the top of the y–axis ("vertical direction")

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

$$r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q \end{cases}$$

projective or affine

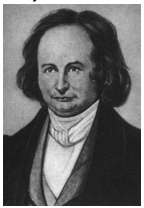
- if $\#(r_{P,Q} \cap E(\mathbb{F}_q)) \geq 2 \;\Rightarrow\; \#(r_{P,Q} \cap E(\mathbb{F}_q)) = 3$

  if tangent line, contact point is counted with multiplicity

- $r_{\infty,\infty} \cap E(\mathbb{F}_q) = \{\infty, \infty, \infty\}$

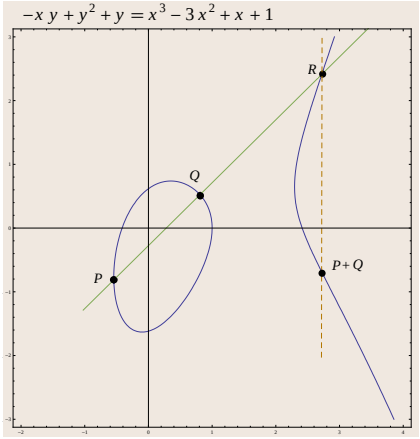
History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity
  $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$



$r_{P,Q} \cap E(\mathbb{F}_q) = \{P, Q, R\}$
$r_{R,\infty} \cap E(\mathbb{F}_q) = \{\infty, R, R'\}$

$$P +_E Q := R'$$

$r_{P,\infty} \cap E(\mathbb{F}_q) = \{P, \infty, P'\}$

$$-P := P'$$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

(a) $P +_E Q \in E(\mathbb{F}_q)$ $\qquad \forall P, Q \in E(\mathbb{F}_q)$

(b) $P +_E \infty = \infty +_E P = P$ $\qquad \forall P \in E(\mathbb{F}_q)$

(c) $P +_E (-P) = \infty$ $\qquad \forall P \in E(\mathbb{F}_q)$

(d) $P +_E (Q +_E R) = (P +_E Q) +_E R$ $\qquad \forall P, Q, R \in E(\mathbb{F}_q)$

(e) $P +_E Q = Q +_E P$ $\qquad \forall P, Q \in E(\mathbb{F}_q)$

- $(E(\mathbb{F}_q), +_E)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- can substitute $\mathbb{F}_q$ with any field K; Theorem holds for $(E(K), +_E)$
- $-P = -(x_1, y_1) = (x_1, -a_1 x_1 - a_3 - y_1)$

Formulas for Addition on E (Summary)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$
  - $x_1 \neq x_2$

  $\Rightarrow$ $P_1 +_E P_2 = \infty$

  $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $2y_1 + a_1x + a_3 = 0$
  - $2y_1 + a_1x + a_3 \neq 0$

  $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$

  $$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x + a_3}, \nu = -\frac{a_3y_1 + x_1^3 - a_4x_1 - 2a_6}{2y_1 + a_1x_1 + a_3}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - a_1\lambda - a_2 - x_1 - x_2, -\lambda^3 - a_1^2\lambda + (\lambda + a_1)(a_2 + x_1 + x_2) - a_3 - \nu)$$

Formulas for Addition on E (Summary for special equation)

$$E : y^2 = x^3 + Ax + B$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$
  - $x_1 \neq x_2$

  $\Rightarrow$ $P_1 +_E P_2 = \infty$

  $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $y_1 = 0$
  - $y_1 \neq 0$

  $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$

  $$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$

Group Structure

Theorem (Classification of finite abelian groups)

If G is abelian and finite, $\exists n_1, \ldots, n_k \in \mathbb{N}^{>1}$ such that

1. $n_1 \mid n_2 \mid \cdots \mid n_k$
2. $G \cong C_{n_1} \oplus \cdots \oplus C_{n_k}$

Furthermore $n_1, \ldots, n_k$ (Group Structure) are unique

Theorem (Structure Theorem for Elliptic curves over a finite field)

Let $E/\mathbb{F}_q$ be an elliptic curve, then

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk} \qquad \exists n, k \in \mathbb{N}^{>0}.$$

(i.e. $E(\mathbb{F}_q)$ is either cyclic ($n = 1$) or the product of 2 cyclic groups)

EXAMPLE: Elliptic curves over $\mathbb{F}_2$ and over $\mathbb{F}_3$

From our previous list:

Groups of points of curves over $\mathbb{F}_2$

E	$E(\mathbb{F}_2)$	$E(\mathbb{F}_2)$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	C_2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	C_4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	C_5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	C_3

Note: each C_i, $i = 1, \ldots, 5$ is represented by a curve $/\mathbb{F}_2$

Groups of points of curves over $\mathbb{F}_3$

i	E_i	$E_i(\mathbb{F}_3)$	$E_i(\mathbb{F}_3)$
1	$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	C_4
2	$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	$C_2 \oplus C_2$
3	$y^2 = x^3 - x + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), (2,1), (2,2)\}$	C_7
4	$y^2 = x^3 - x - 1$	$\{\infty\}$	$\{1\}$
5	$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	C_3
6	$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	C_6
7	$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	C_5
8	$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	C_2

Note: each C_i, $i = 1, \ldots, 7$ is represented by a curve $/\mathbb{F}_3$

The j-invariant

Let $E/K : y^2 = x^3 + Ax + B$, $p \geq 5$ and $\Delta_E := 4A^3 + 27B^2$.

Definition

The j–invariant of E is $j = j(E) = 1728\frac{4A^3}{4A^3+27B^2}$

Definition

Let $u \in K^*$. The elliptic curve $E_u : y^2 = x^3 + u^2Ax + u^3B$ is called the twist of E by u

Properties of j–invariants

1. $j(E) = j(E_u), \forall u \in K^*$
2. $j(E'/K) = j(E''/K) \Rightarrow \exists u \in \overline{K}^*$ s.t. $E'' = E'_u$
3. $j \neq 0, 1728 \Rightarrow E : y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}, j(E) = j$
4. $j = 0 \Rightarrow E : y^2 = x^3 + B, \quad j = 1728 \Rightarrow E : y^2 = x^3 + Ax$
5. $j : K \longleftrightarrow \{\bar{K}$–affinely equivalent classes of $E/K\}$.
6. $p = 2, 3$ different definition
7. E and E_μ are $\mathbb{F}_q[\sqrt{\mu}]$–affinely equivalent
8. $\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2})$
9. usually $\#E(\mathbb{F}_q) \neq \#E_\mu(\mathbb{F}_q)$

Determining points of order 2

Let $P = (x_1, y_1) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

$$P \text{ has order } 2 \iff 2P = \infty \iff P = -P$$

So

$$-P = (x_1, -a_1x_1 - a_3 - y_1) = (x_1, y_1) = P \implies 2y_1 = -a_1x_1 - a_3$$

If $p \neq 2$, can assume $E : y^2 = x^3 + Ax^2 + Bx + C$

$$-P = (x_1, -y_1) = (x_1, y_1) = P \implies y_1 = 0, x_1^3 + Ax_1^2 + Bx_1 + C = 0$$

Note

- the number of points of order 2 in $E(\mathbb{F}_q)$ equals the number of roots of $X^3 + AX^2 + BX + C$ in $\mathbb{F}_q$
- roots are distinct since discriminant $\Delta_E \neq 0$

Determining points of order 2 (continues)

Definition

2–torsion points

$$E[2] = \{P \in E(\overline{\mathbb{F}_q}) : 2P = \infty\}.$$

FACTS:

$$E[2] \cong \begin{cases} C_2 \oplus C_2 & \text{if } p > 2 \\ C_2 & \text{if } p = 2, E : y^2 + xy = x^3 + a_4x + a_6 \\ \{\infty\} & \text{if } p = 2, E : y^2 + a_3y = x^3 + a_2x^2 + a_6 \end{cases}$$

Each curve $/\mathbb{F}_2$ has cyclic $E(\mathbb{F}_2)$.

E	$E(\mathbb{F}_2)$	$\lvert E(\mathbb{F}_2)\rvert$
$y^2 + xy = x^3 + x^2 + 1$	$\{\infty, (0,1)\}$	2
$y^2 + xy = x^3 + 1$	$\{\infty, (0,1), (1,0), (1,1)\}$	4
$y^2 + y = x^3 + x$	$\{\infty, (0,0), (0,1), (1,0), (1,1)\}$	5
$y^2 + y = x^3 + x + 1$	$\{\infty\}$	1
$y^2 + y = x^3$	$\{\infty, (0,0), (0,1)\}$	3

Determining points of order 3

Let $P = (x_1, y_1) \in E(\mathbb{F}_q)$

$$P \text{ has order 3} \iff 3P = \infty \iff 2P = -P$$

So, if $p > 3$ and $E : y^2 = x^2 + Ax + B$

$$2P = (x_{2P}, y_{2P}) = 2(x_1, y_1) = (\lambda^2 - 2x_1, -\lambda^3 + 2\lambda x_1 - \nu) \quad \text{where } \lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}.$$

$$P \text{ has order 3} \iff x_{2P} = \lambda^2 - 2x_1 = x_1$$

Substituting λ,

$$x_{2P} - x_1 = \frac{-3x_1^4 - 6Ax_1^2 - 12Bx_1 + A^2}{4(x_1^3 + Ax_1 + 4B)} = 0$$

Note (Conclusions)

- $\psi_3(x) := 3x^4 + 6Ax^2 + 12Bx - A^2$ called the 3rd *division* polynomial
- $(x_1, y_1) \in E(\mathbb{F}_q)$ has order 3 $\Rightarrow \psi_3(x_1) = 0$
- $E(\mathbb{F}_q)$ has at most 8 points of order 3
- If $p \neq 3$, $E[3] := \{P \in E(\overline{\mathbb{F}_q}) : 3P = \infty\} \cong C_3 \oplus C_3$
- If $p = 3$, $E : y^2 = x^3 + Ax^2 + Bx + C$ and $P = (x_1, y_1)$ has order 3, then
  1. $Ax_1^3 + AC - B^2 = 0$
  2. $E[3] \cong C_3$ if $A \neq 0$ and $E[3] = \{\infty\}$ otherwise

Determining points of order 3 (continues)

FACTS:

$$E[3] \cong \begin{cases} C_3 \oplus C_3 & \text{if } p \neq 3 \\ C_3 & \text{if } p = 3, E : y^2 = x^3 + Ax^2 + Bx + C, A \neq 0 \\ \{\infty\} & \text{if } p = 3, E : y^2 = x^3 + Bx + C \end{cases}$$

Example: inequivalent curves $/\mathbb{F}_7$ with $\#E(\mathbb{F}_7) = 9$.

E	$\psi_3(x)$	$E[3] \cap E(\mathbb{F}_7)$	$E(\mathbb{F}_7) \cong$
$y^2 = x^3 + 2$	$x(x+1)(x+2)(x+4)$	$\{\infty, (0, \pm 3), (-1, \pm 1), (5, \pm 1), (3, \pm 1)\}$	$C_3 \oplus C_3$
$y^2 = x^3 + 3x + 2$	$(x+2)(x^3 + 5x^2 + 3x + 2)$	$\{\infty, (5, \pm 3)\}$	C_9
$y^2 = x^3 + 5x + 2$	$(x+4)(x^3 + 3x^2 + 5x + 2)$	$\{\infty, (3, \pm 3)\}$	C_9
$y^2 = x^3 + 6x + 2$	$(x+1)(x^3 + 6x^2 + 6x + 2)$	$\{\infty, (6, \pm 3)\}$	C_9

One count the number of inequivalent $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = r$

Example (A curve over $\mathbb{F}_4 = \mathbb{F}_2(\xi), \xi^2 = \xi + 1$; $E : y^2 + y = x^3$)

We know $E(\mathbb{F}_2) = \{\infty, (0,0), (0,1)\} \subset E(\mathbb{F}_4)$.

$E(\mathbb{F}_4) = \{\infty, (0,0), (0,1), (1,\xi), (1,\xi+1), (\xi,\xi), (\xi,\xi+1), (\xi+1,\xi), (\xi+1,\xi+1)\}$

$$\psi_3(x) = x^4 + x = x(x+1)(x+\xi)(x+\xi+1) \Rightarrow E(\mathbb{F}_4) \cong C_3 \oplus C_3$$

Determining points of order (dividing) m

Definition (m–torsion point)

Let E/K and let $\overline{K}$ an *algebraic closure of* K.

$$E[m] = \{P \in E(\overline{K}) : \ mP = \infty\}$$

Theorem (Structure of Torsion Points)

Let E/K *and* $m \in \mathbb{N}$. *If* $p = \text{char}(K) \nmid m$,

$$E[m] \cong C_m \oplus C_m$$

If $m = p^r m'$, $p \nmid m'$,

$$E[m] \cong C_m \oplus C_{m'} \qquad \textit{or} \qquad E[m] \cong C_{m'} \oplus C_{m'}$$

$$E/\mathbb{F}_p \text{ is called } \begin{cases} \textit{ordinary} & \text{if } E[p] \cong C_p \\ \textit{supersingular} & \text{if } E[p] = \{\infty\} \end{cases}$$

Group Structure of $E(\mathbb{F}_q)$

Corollary

Let $E/\mathbb{F}_q$. $\exists n, k \in \mathbb{N}$ are such that

$$E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$$

Proof.

From classification Theorem of finite abelian group

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$$

with $n_i | n_{i+1}$ for $i \geq 1$.
Hence $E(\mathbb{F}_q)$ contains n_1^r points of order dividing n_1. From *Structure of Torsion Theorem*, $\#E[n_1] \leq n_1^2$. So $r \leq 2$ □

Theorem (Corollary of Weil Pairing)

Let $E/\mathbb{F}_q$ and $n, k \in \mathbb{N}$ s.t. $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$. Then $n \mid q - 1$.

We shall discuss Weil Pairing Wednesday

The division polynomials

Definition (Division Polynomials of $E : y^2 = x^3 + Ax + B$ ($p > 3$))

$$
\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2 \\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3
\end{aligned}
$$

The polynomial $\psi_m \in \mathbb{Z}[x, y]$ is called the m^{th} *division polynomial*

FACTS:

- $\psi_{2m+1} \in \mathbb{Z}[x]$ and $\psi_{2m} \in 2y\mathbb{Z}[x]$
- $\psi_m = \begin{cases} y(mx^{(m^2-4)/2} + \cdots) & \text{if } m \text{ is even} \\ mx^{(m^2-1)/2} + \cdots & \text{if } m \text{ is odd.} \end{cases}$
- $\psi_m^2 = m^2 x^{m^2-1} + \cdots$

Remark.

- $E[2m+1] \setminus \{\infty\} = \{(x,y) \in E(\bar{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x,y) \in E(\bar{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$

Example

$$\psi_4(x) = 2y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4BAx - A^3 - 8B^2)$$

$$\begin{aligned}\psi_5(x) =& 5x^{12} + 62Ax^{10} + 380Bx^9 - 105A^2x^8 + 240BAx^7 + \left(-300A^3 - 240B^2\right)x^6 - 696BA^2x^5 + \left(-125A^4 - 1920B^2A\right)x^4 \\ &+ \left(-80BA^3 - 1600B^3\right)x^3 + \left(-50A^5 - 240B^2A^2\right)x^2 + \left(-100BA^4 - 640B^3A\right)x + \left(A^6 - 32B^2A^3 - 256B^4\right)\end{aligned}$$

$$\begin{aligned}\psi_6(x) =& 2y(6x^{16} + 144Ax^{14} + 1344Bx^{13} - 728A^2x^{12} + \left(-2576A^3 - 5376B^2\right)x^{10} - 9152BA^2x^9 + \left(-1884A^4 - 39744B^2A\right)x^8 \\ &+ \left(1536BA^3 - 44544B^3\right)x^7 + \left(-2576A^5 - 5376B^2A^2\right)x^6 + \left(-6720BA^4 - 32256B^3A\right)x^5 \\ &+ \left(-728A^6 - 8064B^2A^3 - 10752B^4\right)x^4 + \left(-3584BA^5 - 25088B^3A^2\right)x^3 + \left(144A^7 - 3072B^2A^4 - 27648B^4A\right)x^2 \\ &+ \left(192BA^6 - 512B^3A^3 - 12288B^5\right)x + \left(6A^8 + 192B^2A^5 + 1024B^4A^2\right))\end{aligned}$$

Theorem ($E : Y^2 = X^3 + AX + B$ elliptic curve, $P = (x, y) \in E$)

$$m(x,y) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2(x)}, \frac{\psi_{2m}(x,y)}{2\psi_m^4(x)}\right) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right)$$

where

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$$

FACTS:

- $\phi_m(x) = x^{m^2} + \cdots \qquad \psi_m(x)^2 = m^2 x^{m^2-1} + \cdots \in \mathbb{Z}[x]$
- $\omega_{2m+1} \in y\mathbb{Z}[x], \omega_{2m} \in \mathbb{Z}[x]$
- $\frac{\omega_m(x,y)}{\psi_m^3(x,y)} \in y\mathbb{Z}(x)$
- $\gcd(\psi_m^2(x), \phi_m(x)) = 1$
- $E[2m+1] \setminus \{\infty\} = \{(x,y) \in E(\overline{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x,y) \in E(\overline{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$

Further Reading...


Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.


J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.


John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.


Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.


Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.


Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.


Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.


Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.


Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.